



**White paper**

**Drafted under the European Markets in Crypto-Assets  
Regulation (EU) 2023/114 (MiCA)**

## 00 Table of contents

01 Date of notification.....	9
02 Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114.....	9
03 Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114.....	9
04 Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114 .....	9
05 Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114 .....	9
06 Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114 .....	9
<b>SUMMARY.....</b>	<b>10</b>
07 Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114 .....	10
08 Characteristics of the crypto-asset .....	10
09 .....	11
10 Key information about the offer to the public or admission to trading.....	11
<b><i>Part A - Information about the offeror or the person seeking admission to trading.....</i></b>	<b><i>11</i></b>
A.1 Name .....	11
A.2 Legal form .....	12
A.3 Registered address .....	12
A.4 Head office .....	12
A.5 Registration date.....	12
A.6 Legal entity identifier.....	12
A.7 Another identifier required pursuant to applicable national law .....	12
A.8 Contact telephone number.....	12
A.9 E-mail address .....	12
A.10 Response time (Days).....	13
A.11 Parent company .....	13
A.12 Members of the management body .....	13
A.13 Business activity .....	13
A.14 Parent company business activity.....	13

A.15 Newly established.....	13
A.16 Financial condition for the past three years .....	14
A.17 Financial condition since registration.....	14
<b><i>Part B - Information about the issuer, if different from the offeror or person seeking admission to trading.....</i></b>	<b>14</b>
B.1 Issuer different from offeror or person seeking admission to trading.....	14
B.2 Name .....	14
B.3 Legal form.....	15
B.4 Registered address .....	15
B.5 Head office .....	15
B.6 Registration date.....	15
B.7 Legal entity identifier.....	15
B.8 Another identifier required pursuant to applicable national law .....	15
B.9 Parent company .....	15
B.10 Members of the management body .....	15
B.11 Business activity .....	15
B.12 Parent company business activity .....	16
<b><i>Part C- Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 .....</i></b>	<b>16</b>
C.1 Name .....	16
C.2 Legal form .....	16
C.3 Registered address .....	16
C.4 Head office.....	16
C.5 Registration date .....	16
C.6 Legal entity identifier .....	16
C.7 Another identifier required pursuant to applicable national law .....	17
C.8 Parent company.....	17
C.9 Reason for crypto-Asset white paper Preparation .....	17
C.10 Members of the Management body .....	17

C.11 Operator business activity .....	17
C.12 Parent company business activity .....	17
C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 .....	17
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114 .....	17
<b><i>Part D- Information about the crypto-asset project .....</i></b>	<b>18</b>
D.1 Crypto-asset project name .....	18
D.2 Crypto-assets name.....	18
D.3 Abbreviation .....	18
D.4 Crypto-asset project description .....	18
D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project .....	18
D.6 Utility Token Classification .....	19
D.7 Key Features of Goods/Services for Utility Token Projects .....	19
D.8 Plans for the token .....	19
D.9 Resource allocation .....	20
D.10 Planned use of Collected funds or crypto-assets .....	20
<b><i>Part E - Information about the offer to the public of crypto-assets or their admission to trading.....</i></b>	<b>20</b>
E.1 Public offering or admission to trading .....	20
E.2 Reasons for public offer or admission to trading .....	20
E.3 Fundraising target .....	20
E.4 Minimum subscription goals .....	20
E.5 Maximum subscription goals .....	21
E.6 Oversubscription acceptance .....	21
E.7 Oversubscription allocation.....	21
E.8 Issue price .....	21
E.9 Official currency or any other crypto-assets determining the issue price .....	21
E.10 Subscription fee .....	21
E.11 Offer price determination method .....	21

<b>E.12 Total number of offered/traded crypto-assets .....</b>	<b>21</b>
<b>E.13 Targeted holders .....</b>	<b>22</b>
<b>E.14 Holder restrictions .....</b>	<b>22</b>
<b>E.15 Reimbursement notice .....</b>	<b>22</b>
<b>E.16 Refund mechanism .....</b>	<b>22</b>
<b>E.17 Refund timeline.....</b>	<b>22</b>
<b>E.18 Offer phases .....</b>	<b>22</b>
<b>E.19 Early purchase discount .....</b>	<b>22</b>
<b>E.20 Time-limited offer .....</b>	<b>23</b>
<b>E.21 Subscription period beginning.....</b>	<b>23</b>
<b>E.22 Subscription period end.....</b>	<b>23</b>
<b>E.23 Safeguarding arrangements for offered funds/crypto-Assets .....</b>	<b>23</b>
<b>E.24 Payment methods for crypto-asset purchase.....</b>	<b>23</b>
<b>E.25 Value transfer methods for reimbursement .....</b>	<b>23</b>
<b>E.26 Right of withdrawal.....</b>	<b>23</b>
<b>E.27 Transfer of purchased crypto-assets .....</b>	<b>23</b>
<b>E.28 Transfer time schedule .....</b>	<b>24</b>
<b>E.29 Purchaser’s technical requirements.....</b>	<b>24</b>
<b>E.30 Crypto-asset service provider (CASP) name.....</b>	<b>24</b>
<b>E.31 CASP identifier .....</b>	<b>24</b>
<b>E.32 Placement form.....</b>	<b>24</b>
<b>E.33 Trading platforms name .....</b>	<b>25</b>
<b>E.34 Trading platforms Market identifier code (MIC).....</b>	<b>25</b>
<b>E.35 Trading platforms access .....</b>	<b>25</b>
<b>E.36 Involved costs .....</b>	<b>25</b>
<b>E.37 Offer expenses .....</b>	<b>25</b>
<b>E.38 Conflicts of interest.....</b>	<b>25</b>
<b>E.39 Applicable law .....</b>	<b>26</b>
<b>E.40 Competent court.....</b>	<b>26</b>
<b><i>Part F - Information about the crypto-assets .....</i></b>	<b>26</b>

F.1 Crypto-asset type .....	26
F.2 Crypto-asset functionality .....	26
F.3 Planned application of functionalities .....	26
<i>A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article.....</i>	<i>27</i>
F.4 Type of crypto-asset white paper .....	27
F.5 The type of submission .....	27
F.6 Crypto-asset characteristics .....	27
F.7 Commercial name or trading name.....	27
F.8 Website of the issuer .....	28
F.9 Starting date of the offer to the public or admission to trading .....	28
F.10 Publication date.....	28
F.11 Any other services provided by the issuer.....	28
F.12 Language or languages of the crypto-asset white paper .....	28
F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available .....	28
F.14 Functionally fungible group digital token identifier, where available .....	28
F.15 Voluntary data flag .....	28
F.16 Personal data flag .....	29
F.17 LEI eligibility .....	29
F.18 Home Member State .....	29
F.19 Host Member States .....	29
<i>Part G - Information on the rights and obligations attached to the crypto-assets.....</i>	<i>29</i>
G.1 Purchaser rights and obligations .....	29
G.2 Exercise of rights and obligations .....	30
G.3 Conditions for modifications of rights and obligations .....	30
G.4 Future public offers.....	30
G.5 Issuer retained crypto-assets .....	30
G.6 Utility token classification.....	30

G.7 Key features of goods/services of utility tokens .....	31
G.8 Utility tokens redemption.....	31
G.9 Non-trading request.....	31
G.10 Crypto-assets purchase or sale modalities .....	31
G.11 Crypto-assets transfer restrictions .....	31
G.12 Supply adjustment protocols.....	31
G.13 Supply adjustment mechanisms .....	31
G.14 Token value protection schemes.....	32
G.15 Token value protection schemes description.....	32
G.16 Compensation schemes.....	32
G.17 Compensation schemes description.....	32
G.18 Applicable law .....	32
G.19 Competent court .....	32
<b>Part H – information on the underlying technology .....</b>	<b>33</b>
H.1 Distributed ledger technology (DLT) .....	33
H.2 Protocols and technical standards .....	33
H.3 Technology used .....	34
H.4 Consensus mechanism .....	35
H.5 Incentive mechanisms and applicable fees .....	35
H.6 Use of distributed ledger technology .....	36
H.7 DLT functionality description.....	36
H.8 Audit .....	36
H.9 Audit outcome .....	36
<b>Part I – Information on risks.....</b>	<b>36</b>
I.1 Offer-related risks .....	36
I.2 Issuer-related risks .....	38
I.3 Crypto-assets-related risks .....	39
I.4 Project implementation-related risks.....	41
I.5 Technology-related risks .....	43
I.6 Mitigation measures.....	45

**Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts .....47**

- J.1 Adverse impacts on climate and other environment-related adverse impacts.....47**
- S.1 Name.....47**
- S.2 Relevant legal entity identifier .....47**
- S.3 Name of the crypto-asset .....47**
- S.4 Consensus Mechanism .....47**
- S.5 Incentive Mechanisms and Applicable Fees .....48**
- S.6 Beginning of the period to which the disclosed information relates.....49**
- S.7 End of the period to which the disclosed information relates.....49**
- S.8 Energy consumption .....49**
- S.9 Energy consumption sources and methodologies .....49**

## **01 Date of notification**

2025-09-01

## **02 Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114**

This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

## **03 Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114**

This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 of the European Parliament and of the Council and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.

## **04 Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114**

The crypto-asset referred to in this crypto-asset white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

## **05 Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114**

Not applicable

## **06 Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114**

The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the

deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

## **SUMMARY**

### **07 Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114**

This summary should be read as an introduction to the crypto-asset white paper.

The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone.

The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law.

This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.

### **08 Characteristics of the crypto-asset**

The zkVerify Token (VFY) is the native crypto-asset of the zkVerify network, a blockchain designed for decentralized verification of zero-knowledge proofs in a secure and efficient manner. Holders of zkVerify Tokens may use them to pay transaction fees on the network, participate in staking to help secure the blockchain, and take part in governance by voting on proposals concerning the protocol's development and future direction.

Owning zkVerify Tokens does not give the holder any ownership rights in the zkVerify Foundation or any entitlement to dividends or profits. Instead, the token is aimed to be used within the zkVerify ecosystem itself: it is the medium for paying fees, rewarding validators who maintain the system, and allowing community participation in decision-making.

Participation in staking or governance is voluntary, and holders must use a compatible digital wallet to exercise these rights. The procedures are carried out directly on the zkVerify blockchain: staking involves locking tokens for a period of time to support validators, while governance involves casting votes through the on-chain referendum system.

The rights associated with zkVerify Tokens are defined in the protocol and may evolve through community governance. This means that rules for staking, rewards, fees, or governance processes can change if approved by the zkVerify Token holder community through established voting mechanisms. Any such changes are transparent, recorded on the zkVerify blockchain, and apply equally to all zkVerify Token holders.

## **09**

Not applicable

## **10 Key information about the offer to the public or admission to trading**

The zkVerify Token is intended to be made available for trading on regulated crypto-asset service providers and other applicable centralized and decentralized exchanges that choose to list it. Admission to trading means that purchasers will be able to buy, sell, and exchange VFY on these platforms, subject to the rules and conditions of each service provider.

The zkVerify Foundation itself does not operate an exchange or directly provide trading services. Instead, access to trading will depend on independent platforms that decide to support the zkVerify Token. Purchasers are responsible for ensuring they comply with all applicable laws in their jurisdiction when acquiring or trading zkVerify Tokens.

The level of liquidity, trading activity, and pricing of the zkVerify Token may vary between different trading venues and over time. There is no guarantee of continuous or uniform availability across platforms, and trading conditions remain dependent on market demand and the policies of the exchanges or service providers involved.

## **Part A - Information about the offeror or the person seeking admission to trading**

### **A.1 Name**

zkVerify Foundation

## **A.2 Legal form**

K575 Cayman Islands foundation company (please refer to the [LEI](#) for more information)

## **A.3 Registered address**

Elgin Court, Elgin Avenue George Town, Grand Cayman KY1-1106, Cayman Islands (please refer to the [LEI](#) for more information)

## **A.4 Head office**

Elgin Court, Elgin Avenue George Town, Grand Cayman KY1-1106, Cayman Islands (please refer to the [LEI](#) for more information)

## **A.5 Registration date**

2024-07-19

## **A.6 Legal entity identifier**

254900YN0N9Y7NYQTF19

## **A.7 Another identifier required pursuant to applicable national law**

Not applicable

## **A.8 Contact telephone number**

+1 (345) 527-4000

## **A.9 E-mail address**

[info@zkverify.io](mailto:info@zkverify.io)

### **A.10 Response time (Days)**

007

### **A.11 Parent company**

Not applicable as there is no parent company (please refer to the [LEI](#) for more information)

### **A.12 Members of the management body**

<b>Name</b>	<b>Business address</b>	<b>Function</b>
Craig Pascoe	340 Andre DR, George Town, Grand Cayman, Cayman Islands, KY1-1106	Director

### **A.13 Business activity**

The zkVerify Foundation is responsible for maintaining, governing and supporting of the zkVerify protocol. Its primary activity is thus to support and govern this decentralized Layer 1 relay chain designed specifically for zero-knowledge proof verification.

The zkVerify Foundation's work includes designing, implementing, and upgrading the zkVerify protocol's infrastructure in order to ensure security, scalability, and efficiency in the verification of zero-knowledge proofs. In addition to technical development, the zkVerify Foundation will aim to facilitate ecosystem growth and governance by enabling community participation in protocol decision-making, allowing for adoption among developers, and supporting projects that choose to build on the zkVerify protocol.

### **A.14 Parent company business activity**

Not applicable

### **A.15 Newly established**

Yes

## **A.16 Financial condition for the past three years**

Not applicable

## **A.17 Financial condition since registration**

The zkVerify Foundation has been established within the past three years and, as such, its financial history is limited. The zkVerify Foundation itself has not raised funds directly and has not needed to do so. Instead, Ellipsis Distributed Systems, Inc. (EDS), an independent development entity, has been responsible for raising and disbursing funds for the design and implementation of the zkVerify protocol. To date, EDS has raised approximately USD 3.5 million through the issuance of token warrants at a USD 60 million valuation. These funds have been allocated primarily to protocol development, including the architecture, testing, and preparation of the Layer 1 Relay Chain of zkVerify.

The zkVerify Foundation's role is to receive and steward the zkVerify technology once development has been completed by EDS, and to maintain the network thereafter. Accordingly, zkVerify Foundation's financial condition reflects its early stage of operations: it has limited direct financial activity to date and no published audited financial statements. Looking forward, its treasury and resources will be managed transparently in line with its governance framework, with expenditures directed towards protocol maintenance, community support and ecosystem development once assuming operational responsibility.

## **Part B - Information about the issuer, if different from the offeror or person seeking admission to trading**

### **B.1 Issuer different from offeror or person seeking admission to trading**

No

### **B.2 Name**

Not applicable

**B.3 Legal form**

Not applicable

**B.4 Registered address**

Not applicable

**B.5 Head office**

Not applicable

**B.6 Registration date**

Not applicable

**B.7 Legal entity identifier**

Not applicable

**B.8 Another identifier required pursuant to applicable national law**

Not applicable

**B.9 Parent company**

Not applicable

**B.10 Members of the management body**

Not applicable

**B.11 Business activity**

Not applicable

## **B.12 Parent company business activity**

Not applicable

## **Part C- Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114**

### **C.1 Name**

Not applicable

### **C.2 Legal form**

Not applicable

### **C.3 Registered address**

Not applicable

### **C.4 Head office**

Not applicable

### **C.5 Registration date**

Not applicable

### **C.6 Legal entity identifier**

Not applicable

**C.7 Another identifier required pursuant to applicable national law**

Not applicable

**C.8 Parent company**

Not applicable

**C.9 Reason for crypto-Asset white paper Preparation**

Not applicable

**C.10 Members of the Management body**

Not applicable

**C.11 Operator business activity**

Not applicable

**C.12 Parent company business activity**

Not applicable

**C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114**

Not applicable

**C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114**

Not applicable

## **Part D- Information about the crypto-asset project**

### **D.1 Crypto-asset project name**

zkVerify

### **D.2 Crypto-assets name**

zkVerify Token

### **D.3 Abbreviation**

VFY

### **D.4 Crypto-asset project description**

zkVerify is a blockchain protocol built as a Substrate-based Layer 1 relay chain that specializes in decentralized verification of zero-knowledge proofs. Zero-knowledge proofs allow for one party to demonstrate that a computation or statement is correct without revealing the underlying data behind said computation or statement. This capability enables new forms of trustless interactions, such as proving results of complex computations or selectively disclosing information, while simultaneously preserving privacy.

The zkVerify protocol is designed to process different types of zero-knowledge proofs efficiently, including advanced proof systems such as STARKs. By providing optimized infrastructure for verification, zkVerify lowers the barriers for developers and applications that rely on proof-based security. Potential use cases span across artificial intelligence, supply chain management, decentralized science and gaming, extending everywhere where verifiable computation and data integrity are critical.

### **D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project**

Name	Role	Domicile
------	------	----------

zkVerify Foundation & DAO	Oversight and governance	Cayman Islands
Ellipsis Distributed Systems, Inc.	Primary blockchain development	United States
Horizen Labs, Inc.	Zero-knowledge expertise and contributions	United States
Pristine Compliance Solutions Ltd	This white paper and MiCA-compliance	Finland

## D.6 Utility Token Classification

No

## D.7 Key Features of Goods/Services for Utility Token Projects

Not applicable

## D.8 Plans for the token

The zkVerify project is being developed to provide a decentralized Layer 1 network specialized in the verification of zero-knowledge proofs. Since its inception, the project has focused on building the technical foundations of the protocol, including the relay chain architecture, the first implementations of proof verifiers, and the design of the on-chain governance system. Early milestones have included the establishment of the zkVerify Foundation, initial fundraising through token warrants (by Ellipsis Distributed Systems, Inc.), and the development of testnet infrastructure to validate core protocol functions.

Future milestones for zkVerify include the launch of the mainnet, the introduction of staking mechanisms to secure the network and reward participants, and the implementation of on-chain governance that allows token holders to take part in decision-making about protocol upgrades and network parameters. In addition, the network will integrate a system for fee payments linked to proof verification, which is intended to sustain the protocol's economics.

## **D.9 Resource allocation**

The zkVerify Foundation has allocated its initial financial resources primarily to protocol development and ecosystem formation. Funds have been directed towards core engineering work, including the design and implementation of the Layer 1 relay chain, the development of proof verifiers, and the establishment of the testnet environment. In addition to protocol engineering, resources have been committed to community building, governance design, and operational infrastructure necessary for sustaining the zkVerify Token and protocol.

## **D.10 Planned use of Collected funds or crypto-assets**

Not applicable as this white paper relates to seeking admission to trading and thus no funds or crypto-assets are going to be collected via a public offer at this stage.

# **Part E - Information about the offer to the public of crypto-assets or their admission to trading**

## **E.1 Public offering or admission to trading**

ATTR (admission to trading)

## **E.2 Reasons for public offer or admission to trading**

Admission to trading is sought in order to increase the liquidity of the zkVerify Token and to allow for more ecosystem participation via increased avenues of access.

## **E.3 Fundraising target**

Not applicable (as this is not a public offer)

## **E.4 Minimum subscription goals**

Not applicable (as this is not a public offer)

### **E.5 Maximum subscription goals**

Not applicable (as this is not a public offer)

### **E.6 Oversubscription acceptance**

Not applicable (as this is not a public offer)

### **E.7 Oversubscription allocation**

Not applicable (as this is not a public offer)

### **E.8 Issue price**

Not applicable (as this is not a public offer)

### **E.9 Official currency or any other crypto-assets determining the issue price**

Not applicable (as this is not a public offer)

### **E.10 Subscription fee**

Not applicable (as this is not a public offer)

### **E.11 Offer price determination method**

Not applicable (as this is not a public offer)

### **E.12 Total number of offered/traded crypto-assets**

1 000 000 000 (i.e. 1 billion). During its launch, 1 billion zkVerify Tokens are minted, all of which are sought to be admitted to trading. However, due to the zkVerify protocol's inflationary mechanics, approximately 30 million new zkVerify Tokens are minted annually. These new tokens are fungible with the initial 1 billion zkVerify Tokens and as such they are also subject to this white paper and their admission to trading is sought automatically.

For more information on the supply adjustment, please refer to Sections [G.12](#) and [G.13](#).

### **E.13 Targeted holders**

ALL (all types of investors)

### **E.14 Holder restrictions**

There are no direct technical restrictions on who may hold zkVerify Tokens. However, all holders remain responsible for ensuring compliance with the laws and regulations applicable in their respective jurisdictions. In addition, crypto-asset service providers, such as exchanges or custodians, may impose their own eligibility requirements or restrictions that can affect access to the tokens. From a technical perspective, holding zkVerify Tokens requires the use of a digital wallet that is compatible with the zkVerify protocol. Beyond this, the zkVerify Foundation does not impose restrictions on the type of holders.

### **E.15 Reimbursement notice**

Not applicable (as this is not a public offer)

### **E.16 Refund mechanism**

Not applicable (as this is not a public offer)

### **E.17 Refund timeline**

Not applicable (as this is not a public offer)

### **E.18 Offer phases**

Not applicable (as this is not a public offer)

### **E.19 Early purchase discount**

Not applicable (as this is not a public offer)

## **E.20 Time-limited offer**

Not applicable (as this is not a public offer)

## **E.21 Subscription period beginning**

Not applicable (as this is not a public offer)

## **E.22 Subscription period end**

Not applicable (as this is not a public offer)

## **E.23 Safeguarding arrangements for offered funds/crypto-Assets**

Not applicable (as this is not a public offer)

## **E.24 Payment methods for crypto-asset purchase**

The methods of payment available for acquiring zkVerify Tokens depend on the crypto-asset service provider or decentralized exchange through which the purchase is made. Different platforms may support various payment options, including other crypto-assets or, where applicable, fiat currency. The zkVerify Foundation itself does not directly facilitate token sales and does not prescribe or limit the payment methods accepted by service providers.

## **E.25 Value transfer methods for reimbursement**

Not applicable (as this is not a public offer)

## **E.26 Right of withdrawal**

Not applicable (as this is not a public offer)

## **E.27 Transfer of purchased crypto-assets**

The zkVerify Tokens are transferred to holders through the zkVerify protocol network. Once purchased via a crypto-asset service provider or decentralized exchange, the zkVerify Tokens

are delivered to the buyer's digital wallet address that is compatible with the zkVerify protocol. Transfers are recorded on-chain, ensuring transparency and verifiability.

The zkVerify Foundation does not directly handle or intermediate token transfers. The process is executed either by the relevant service provider facilitating the purchase or through decentralized exchanges, with final settlement occurring on the zkVerify protocol.

### **E.28 Transfer time schedule**

Not applicable (as this is not a public offer)

### **E.29 Purchaser's technical requirements**

Holders of zkVerify Tokens are generally only required to possess a digital wallet that is compatible with the zkVerify protocol. No additional technical requirements are imposed by the zkVerify Foundation itself. However, crypto-asset service providers or exchanges where zkVerify Tokens may be listed could impose specific technical requirements for holding, transferring, or interacting with the tokens. Such requirements, which may include supported wallet types, minimum software versions, or additional security protocols, are determined solely by the respective service providers and are outside the control of the zkVerify Foundation. Prospective purchasers are responsible for ensuring that their chosen wallet or service provider meets all technical requirements for purchasing zkVerify Tokens.

### **E.30 Crypto-asset service provider (CASP) name**

Not applicable. There is no CASP appointed or mandated for placing of VFY.

### **E.31 CASP identifier**

Not applicable. There is no CASP appointed or mandated for placing of VFY.

### **E.32 Placement form**

NTAV – Not applicable

### **E.33 Trading platforms name**

No specific trading platforms are designated at the time of drafting this white paper. Admission to trading is sought on all trading platforms compliant with MiCA.

### **E.34 Trading platforms Market identifier code (MIC)**

This depends on the trading platform listing the asset.

### **E.35 Trading platforms access**

Access conditions will depend on the trading platforms that may list the zkVerify Token.

### **E.36 Involved costs**

Costs, if any, will depend on the trading platforms that may list the zkVerify Token. Such costs may include transaction or withdrawal fees charged by the platform itself or network fees incurred when transferring zkVerify Tokens off-platform.

### **E.37 Offer expenses**

Not applicable (as this is not a public offer)

### **E.38 Conflicts of interest**

The zkVerify Foundation holds approximately 31.375% of the initial supply of zkVerify Tokens. This significant holding could give rise to potential conflicts of interest, as the zkVerify Foundation's financial incentives may, in certain circumstances, diverge from those of other token holders. For example, the zkVerify Foundation could be in a position to influence token markets, governance decisions, or the timing of certain initiatives in a way that benefits its own holdings. In addition, other persons, including founders, employees, and advisors of the zkVerify Foundation, may hold zkVerify Tokens or other financial interests linked to the success of the project. These holdings could create situations where their personal or financial interests potentially conflict with the interests of other token holders.

The zkVerify Foundation aims to manage and mitigate such conflicts through transparent governance practices, disclosures, and adherence to applicable legislation. Nevertheless, prospective purchasers should be aware that these potential conflicts of interest exist.

### **E.39 Applicable law**

Not applicable (as this is not a public offer and this field applies to public offers only)

### **E.40 Competent court**

For any disputes arising out of or in connection with the admission to trading of zkVerify Tokens, the competent courts of Germany shall have exclusive jurisdiction.

## **Part F - Information about the crypto-assets**

### **F.1 Crypto-asset type**

A crypto-asset other than an electronic money token or an asset referenced token that does not qualify as a financial instrument or otherwise fall outside the scope of MiCA.

### **F.2 Crypto-asset functionality**

zkVerify is an open-source protocol, primarily implemented in Rust and developed using Parity's Substrate framework. The zkVerify Token serves as the native token within the zkVerify protocol's network and has the following core functions:

- **Staking:** Token holders may stake zkVerify Tokens to help secure the network and participate in its consensus mechanism in order to gain yield on their staked tokens.
- **Governance:** Token holders may take part in protocol governance, including voting on proposals related to network upgrades, parameter changes, and other key decisions.
- **Transaction and verification fees:** The zkVerify Tokens are used to pay fees for zero-knowledge proof verification and other transactions executed within the network.

### **F.3 Planned application of functionalities**

All of the current functionalities, as outlined above, are already in use within the zkVerify testnet, and will be instantly available in the mainnet as well once it launches during Q3 of

2025. Any further future developments and application of functionalities cannot easily be predicted due to the decentralized governance structure of the zkVerify protocol.

**A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article**

**F.4 Type of crypto-asset white paper**

OTHR

**F.5 The type of submission**

NEWT

**F.6 Crypto-asset characteristics**

The zkVerify Token is the native foundational token of the zkVerify protocol. It is a fungible digital asset issued on a blockchain built with Parity's Substrate framework and designed to support the verification of zero-knowledge proofs in a secure and efficient manner. The token enables participants to access and use core functions of the network, including staking to contribute to network security, participating in on-chain governance processes, and paying transaction and verification fees. The zkVerify Token is freely transferable between compatible digital wallets, subject to applicable legal and regulatory requirements, and it forms the foundation for the economic incentives that sustain the zkVerify ecosystem.

**F.7 Commercial name or trading name**

Not applicable (please refer to the DTI for this information)

**F.8 Website of the issuer**

<https://zkverify.io>

**F.9 Starting date of the offer to the public or admission to trading**

2025-10-15

**F.10 Publication date**

2025-10-15

**F.11 Any other services provided by the issuer**

Not applicable

**F.12 Language or languages of the crypto-asset white paper**

English

**F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available**

4NLNNX12F

**F.14 Functionally fungible group digital token identifier, where available**

Not applicable

**F.15 Voluntary data flag**

Not applicable (as this is not a public offer and this field applies only to public offers)

## **F.16 Personal data flag**

Yes

## **F.17 LEI eligibility**

eligible

## **F.18 Home Member State**

Germany

## **F.19 Host Member States**

Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

# **Part G - Information on the rights and obligations attached to the crypto-assets**

## **G.1 Purchaser rights and obligations**

Purchasers of zkVerify Tokens acquire the right to use the tokens within the zkVerify protocol. This includes the ability to stake tokens in order to participate in network security and to receive potential staking rewards, as well as the right to take part in governance processes by voting on proposals concerning protocol upgrades, parameter changes, or other decisions affecting the network. Purchasers may also use zkVerify Tokens to pay transaction and verification fees within the network. Purchasers do not obtain ownership rights, equity interests, or claims against the zkVerify Foundation or any related entity. The rights of purchasers are limited to the use of the zkVerify Token as defined by the protocol.

Token holders are expected to act honestly and in good faith when interacting with the zkVerify protocol and when exercising governance rights. In addition, they remain responsible for complying with all applicable legal, tax, and regulatory obligations.

## **G.2 Exercise of rights and obligations**

The rights associated with zkVerify Tokens, such as staking, participation in governance, and payment of fees, are exercised directly on the zkVerify blockchain. Purchasers may exercise these rights by using a compatible digital wallet that supports interaction with the zkVerify protocol. Access to these rights is conditional upon the holder maintaining control of their zkVerify Tokens within such a wallet and complying with the technical and security requirements necessary to interact with the network. The exercise of governance rights further requires participation in on-chain voting processes conducted through the protocol.

## **G.3 Conditions for modifications of rights and obligations**

The rights and obligations attached to zkVerify Tokens may be modified exclusively through the protocol's decentralized governance process. Token holders may propose and vote on changes via on-chain governance mechanisms. Any modification requires approval by the community in accordance with the governance rules defined within the zkVerify protocol. The zkVerify Foundation does not and cannot unilaterally alter the rights or obligations of token holders; such changes are determined collectively by the decentralized autonomous organization (DAO) through transparent and verifiable voting procedures.

## **G.4 Future public offers**

Not applicable as none are planned currently. If a public offer were to be conducted in the future, it would likely be provisioned by the zkVerify DAO.

## **G.5 Issuer retained crypto-assets**

Although technically the zkVerify Tokens are issued by the zkVerify blockchain itself and therefore they do not have a direct issuer, in this case the zkVerify Foundation's holdings should still be disclosed. zkVerify Foundation retains 313 750 000 zkVerify Tokens.

## **G.6 Utility token classification**

No

## **G.7 Key features of goods/services of utility tokens**

Not applicable

## **G.8 Utility tokens redemption**

Not applicable

## **G.9 Non-trading request**

Admission to trading is sought.

## **G.10 Crypto-assets purchase or sale modalities**

Not applicable as the admission to trading of the tokens is sought.

## **G.11 Crypto-assets transfer restrictions**

The zkVerify Tokens are generally freely transferable between holders using compatible digital wallets and/or supported crypto-asset service providers or other trading venues. The zkVerify protocol itself does not impose restrictions on the transferability of the tokens. However, transferability may be limited in certain circumstances by applicable legal and regulatory requirements in specific jurisdictions, or by the technical or compliance policies of third-party service providers, such as crypto-asset service providers. Purchasers shall remain solely responsible for ensuring that any transfer, use, or holding of zkVerify Tokens complies with the laws and regulations of the jurisdiction in which they are located in.

## **G.12 Supply adjustment protocols**

Yes

## **G.13 Supply adjustment mechanisms**

The supply of zkVerify Tokens is subject to an inflationary mechanism designed to incentivize network security and ecosystem growth. Initially, new tokens will be issued at an annual rate of approximately 3%, corresponding to around 30 000 000 new tokens per year. Of the newly

minted tokens, approximately 85% are distributed as rewards to stakers who contribute to securing the network, while the remaining 15% are allocated to the on-chain treasury to fund ecosystem development. This issuance model is governed by the protocol's on-chain governance system. Token holders may propose and vote on changes to parameters such as the inflation rate, staking reward distribution, or treasury allocation. There is no fixed maximum token supply; instead, issuance is algorithmically determined and may evolve over time in accordance with governance decisions made by the community.

#### **G.14 Token value protection schemes**

No

#### **G.15 Token value protection schemes description**

Not applicable

#### **G.16 Compensation schemes**

No

#### **G.17 Compensation schemes description**

Not applicable

#### **G.18 Applicable law**

The laws of the Federal Republic of Germany.

#### **G.19 Competent court**

The competent court of first instance shall be the Frankfurt am Main Local Court. Contact details of the competent court:

Address: Gerichtsstraße 2 60313 Frankfurt am Main

Phone number: +49 (0) 69 1367 01

## **Part H – information on the underlying technology**

### **H.1 Distributed ledger technology (DLT)**

The zkVerify protocol is built on purpose-designed distributed ledger technology using the Substrate framework. The underlying technology stack of Polkadot has been developed from the ground up (primarily in Rust via the Substrate framework) and is distinct from legacy blockchains, though it draws on proven principles of cryptographic and distributed systems.

At its core, the zkVerify protocol operates as a public, permissionless blockchain known as the Relay Chain. The Relay Chain coordinates a decentralized set of validators who maintain consensus over the state of the network. The zkVerify blockchain records token balances, accounts, governance actions, staking information, and the metadata needed to support parachains (such as parachain block headers, cross-chain message queues, staking information, governance referenda, etc.). For efficiency, the Relay Chain itself has minimal functionality and does not record arbitrary smart contract code.

Parachains connected to zkVerify blockchain maintain their own ledgers, which are embedded into the Relay Chain's state through cryptographic proofs and consensus. This design allows the zkVerify protocol to function as a sharded ledger system, where each parachain operates independently but benefits from shared security and interoperability.

Transactions within the zkVerify blockchain are signed using modern cryptographic standards (Sr25519, a variant of Ed25519 optimized for Substrate) and propagated across a peer-to-peer network. Consensus ensures that all valid transactions are included in blocks, each cryptographically linked to the previous, thus forming an immutable blockchain. The Relay Chain also guarantees consistency for cross-chain operations by finalizing blocks in a way that ensures atomicity – meaning that multi-chain transactions either succeed entirely or fail without partial execution.

### **H.2 Protocols and technical standards**

The zkVerify blockchain employs a hybrid consensus mechanism that combines BABE (Blind Assignment for Blockchain Extension) for block production with GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) for finality.

BABE is a Proof-of-Stake –based protocol that uses a lottery mechanism to determine which validator may produce the next block. The probability of being selected is weighted by the amount of the validator’s stake, similar in design to the Ouroboros protocol used by Cardano. This ensures continuous block production and fair participation among validators.

GRANDPA, by contrast, provides strong finality. It is a Byzantine Fault Tolerant (BFT) protocol in which validators vote on the “head” of the chain. Once at least two-thirds of the validators attest to a specific chain, all blocks up to that point are finalized and cannot be reverted. This separation between block production (with BABE) and finality (with GRANDPA) enables the zkVerify blockchain to achieve both efficiency and strong security guarantees.

The consensus mechanism of zkVerify is designed to be robust and secure under standard fault tolerance assumptions. It can tolerate up to one-third of validators behaving maliciously without losing finality, which is the standard threshold for BFT protocols. If more than one-third, but fewer than half of, validators act maliciously, block finality may temporarily halt. However, BABE can continue producing blocks with probabilistic finality until GRANDPA resumes. In the extreme case where an attacker would control a majority of stake (i.e. 51% or more), they could disrupt consensus. To counter this, zkVerify incorporates economic safeguards – most notably slashing of misbehaving validators’ stakes – which impose severe financial penalties on malicious actors, thereby deterring such attacks.

To further strengthen security, zkVerify organizes consensus participation into sessions: short intervals during which validator assignments and responsibilities are rotated. This frequent rotation of GRANDPA authorities makes it significantly harder for an adversary to predict or corrupt validator sets, enhancing both decentralization and resilience.

### **H.3 Technology used**

Security is a central element of zkVerify’s design. All parachains connected to the zkVerify network benefit from the shared security provided by the Relay Chain’s validator set. Unlike typical standalone blockchains that must independently recruit and secure their own validator or miner communities, zkVerify uses a pooled security model: as long as the Relay Chain remains secure, every parachain intrinsically inherits that security.

This model is implemented through Nominated Proof-of-Stake (NPoS) consensus. In NPoS, holders of the zkVerify Token can participate in securing the network by nominating validators with their stake. Validators are then selected based on nominations, with a rotating set of the highest-ranked validators producing blocks and validating parachain transactions. This system is designed to maximize both decentralization and security.

By enabling many different token holders to participate in nominating validators, NPoS promotes a broad distribution of stake across the entire network, reducing concentration of power. Simultaneously, the economic incentives for validators and nominators – through staking rewards and penalties (i.e. slashing) for misconduct – align the interests of participants with the integrity of the network. Through this combination of pooled security, validator rotation, and incentive alignment, the zkVerify protocol ensures that the Relay Chain and its parachains operate on a maximally secure and decentralized foundation.

#### **H.4 Consensus mechanism**

Please refer to Section [H.2](#) above.

#### **H.5 Incentive mechanisms and applicable fees**

As mentioned in Section [H.3](#) above, the zkVerify blockchain secures transactions through a NPoS consensus mechanism. In this system, validators are responsible for producing blocks and verifying transactions, while nominators (i.e. the token holders who delegate their stake to validators) support the validator set and share in the rewards.

Validators earn token rewards through a combination of inflationary issuance and a share of collected transaction fees. Nominators receive a proportional share of these rewards based on the performance of the validators they support. To preserve network integrity, the protocol applies slashing penalties in cases of malicious activity, such as double-signing or collusion, as well as for prolonged validator downtime. Both validators and their nominators are subject to these penalties, aligning incentives toward honest and reliable participation.

Transaction fees, paid in zkVerify Tokens, are calculated using a weight-based fee model. Each transaction includes a base fee, an additional fee determined by the computational complexity (weight) of the transaction, and a size-related fee based on the number of bytes transmitted. Fees are dynamically adjusted by a congestion multiplier, which increases or decreases costs depending on current network demand. This mechanism helps prevent spam, ensures throughput efficiency, and maintains predictable network performance.

A portion of collected fees is allocated to the zkVerify Treasury, which supports ecosystem development, protocol maintenance, and governance initiatives. All incentive and fee structures are embedded directly into the protocol logic, ensuring transparent and decentralized distribution without reliance on centralized control.

## **H.6 Use of distributed ledger technology**

No, DLT not operated by the issuer or a third-party acting on the issuer's behalf

## **H.7 DLT functionality description**

Not applicable

## **H.8 Audit**

Yes

## **H.9 Audit outcome**

Audit was conducted by Trail of Bits. No critical issues were found and the zkVerify protocol was deemed as secure. Please find the audit here:

<https://github.com/trailofbits/publications/blob/master/reviews/2025-02-zkverify-foundation-blockchain-securityreview.pdf>.

## **Part I – Information on risks**

### **I.1 Offer-related risks**

#### **1. Market volatility**

The price of the zkVerify Token is determined by supply and demand dynamics on global markets and trading venues. Crypto-assets are typically subject to extreme price fluctuations, which may be driven by overall market sentiment, macroeconomic factors, regulatory announcements, or events specific to the crypto sector. Sudden and/or significant price swings could result in financial losses for zkVerify Token holders.

#### **2. Inflation and token dilution**

The zkVerify Token has an annual supply increase of up to 3%, subject to governance adjustments. This inflation is used to fund staking rewards and the treasury, thereby supporting network security and growth. However, those zkVerify Token holders who do not participate in staking or other network activities may experience dilution of their holdings

relative to the total supply. If network adoption and demand fail to match the inflation rate, downward pressure on zkVerify Token value could occur.

### **3. Regulatory uncertainty**

The legal and regulatory treatment of crypto-assets remains uncertain and varies significantly across jurisdictions. While MiCA is generally expected to harmonize rules within the European Union, global regulatory approaches differ and may impose restrictions on trading, custody, or use of zkVerify Tokens. Future changes in legislation or regulatory enforcement could negatively impact zkVerify Token's tradability and value.

### **4. Competition and adoption**

zkVerify operates in a competitive landscape where other protocols are pursuing similar goals in zero-knowledge proof verification. Alternative solutions – such as those based on Cosmos or other blockchain ecosystems – may capture developer or user interest. If zkVerify fails to achieve sufficient adoption, demand for the zkVerify Token could stagnate or decline.

### **5. Operational and technical**

As with any blockchain infrastructure, zkVerify faces operational risks, including potential network outages, transaction delays, or forks. High transaction volumes, malicious spam, or unforeseen vulnerabilities could strain the system. Despite rigorous testing, software bugs or exploits could still occur, impacting network reliability or token holder assets.

### **6. Liquidity**

Liquidity of the zkVerify Tokens on trading venues cannot be guaranteed. Limited trading volumes may result in high price volatility or difficulty entering and exiting positions at desired prices. Different venues may also impose varying restrictions, such as withdrawal limits or limits on order types, which could affect liquidity.

### **7. Smart contracts and integration**

Although zkVerify's Relay Chain minimizes reliance on arbitrary smart contracts, parachains, bridges, and integrations may introduce vulnerabilities. Exploits of third-party code or integration errors could have knock-on effects for holders or the broader ecosystem.

### **8. Key-personnel and project sustainability**

As a project in its early stages, zkVerify relies on continued development by its core contributors and the stewardship of the zkVerify Foundation. Loss of key personnel, insufficient funding, or failure to achieve sufficient ecosystem growth could adversely impact the long-term sustainability of the zkVerify protocol.

## **I.2 Issuer-related risks**

Contrary to traditional financial instruments, the zkVerify Tokens do not have a central corporate issuer. This eliminates certain conventional risks – such as corporate insolvency – but introduces risks specific to decentralized networks and their supporting institutions.

### **1. Decentralization and lack of central accountability**

As the zkVerify Tokens have no central issuer, there is no single entity obligated to guarantee their value, performance, or continued development. If network issues arise, there is no central authority that can be held accountable or compelled to act. Instead, the network relies on open-source contributors and community participation. A decline in developer engagement or ecosystem funding could slow innovation and reduce competitiveness.

### **2. Dependence on the zkVerify Foundation and core developers**

Although decentralized in operation, zkVerify's early-stage deployment is strongly supported by the zkVerify Foundation. If the zkVerify Foundation were to encounter financial distress, legal actions, internal disputes, or dissolution, project development could be disrupted. Similarly, the loss of key developers or leadership changes may delay upgrades, weaken strategic direction, or erode market confidence. While community contributions can sustain the project, the departure of experienced personnel poses material risks.

### **3. Regulatory and legal risks for supporting entities**

While the zkVerify Tokens themselves function within a decentralized network, entities such as the zkVerify Foundation may be subject to legal or regulatory actions. Such actions could affect the zkVerify Foundation's ability to support development, manage resources, or coordinate community governance, potentially slowing the project's progress.

### **4. Governance risk and potential for forks**

Protocol changes are determined through decentralized governance. While this strengthens transparency, it also carries risks: disagreements among stakeholders could slow decision-making or, in extreme cases, result in contentious network forks (chain splits). Forks can create uncertainty for holders and reduce confidence in the stability of the ecosystem.

### **5. Validator concentration risks**

The zkVerify protocol's security depends on a sufficiently decentralized validator set. If a significant portion of staking power concentrates in a few validators or pools, these entities

could exert disproportionate influence over governance decisions or block production. This centralization would reduce the resilience and neutrality of the network.

## **6. Operational and infrastructure risks**

Because the zkVerify protocol lacks formal corporate governance, there are no contractual service-level guarantees for network operations. Supporting infrastructure such as explorers, governance portals, or official websites may face downtime or cyberattacks. In the event of critical bugs, decentralized coordination may delay fixes compared to centralized systems where issuers or governing entities can push mandatory updates.

## **7. Funding continuity risks**

The project's early development relies heavily on funds raised and managed by the zkVerify Foundation. If treasury resources are depleted quicker than anticipated, or if new sources of funding are not secured, the long-term sustainability of zkVerify could be challenged.

## **8. Reputational risks**

As an emerging protocol in a competitive environment, zkVerify is exposed to reputational risks stemming from technical failures, governance disputes, or negative regulatory actions against associated entities. Any such events could reduce adoption and undermine trust.

# **I.3 Crypto-assets-related risks**

## **1. Market volatility and price**

The value of the zkVerify Tokens is determined entirely by supply and demand in the market. There is no guarantee of stability, and prices may rise or fall sharply within short periods. Holders face the risk of losing a substantial portion, or even all, of their investment due to adverse market movements or other volatilities affecting the crypto sphere.

## **2. Lack of intrinsic value**

The zkVerify Tokens are not backed by physical assets, government guarantees, or redemption rights. Its value derives primarily from its utility within the zkVerify network (e.g. staking, transaction fees, governance) and from network adoption. If demand for these functions does not develop as anticipated, or if competing assets become preferred alternatives, the market value of zkVerify Tokens could decline significantly.

## **3. Liquidity and exchange availability**

While the zkVerify Tokens are intended to be traded on multiple exchanges and trading venues, liquidity cannot be guaranteed. Regulatory restrictions, exchange policies, or market disruptions may limit where and how zkVerify Tokens can be traded. In stressed market conditions, trading volumes could decrease sharply, making it difficult for holders to convert tokens into fiat or other assets without significant price impact.

#### **4. Custody and key management**

Owning and holding zkVerify Tokens requires secure management of cryptographic keys. Holders who self-custody and lose access to their private keys or seed phrases will permanently lose access. For tokens held through custodial service providers, holders face counterparty risks, including insolvency, fraud, or technical failure at the custodian.

#### **5. Regulation and taxation**

Legal treatment of crypto-assets varies by jurisdiction and is subject to change. Future regulation may restrict trading, use, or transfer of zkVerify Tokens. In addition, token holders may be subject to taxation (e.g. capital gains, income, or VAT) on holdings or transactions. Unclear or inconsistent tax regimes may create additional compliance burdens.

#### **6. Network security and technology**

Although zkVerify is designed with advanced distributed ledger technology, risks remain. Undiscovered software bugs, vulnerabilities in consensus, or targeted attacks could disrupt the network or undermine confidence. Exploitation of related infrastructure – such as parachains, bridges, or integrations – could also negatively affect token value and usability.

#### **7. Competition alternative ecosystems**

zkVerify operates in a highly competitive environment. Alternative protocols compete for the same developer and user base. If zkVerify fails to achieve sufficient adoption or if competitors capture its target niche, demand for the zkVerify Tokens could stagnate.

#### **8. Sustainability of staking rewards**

Validator incentives are currently supported by inflationary token issuance. Over time, the protocol is designed to shift more toward fee-based rewards. If network usage and fee revenue do not scale as anticipated, while inflation decreases, validator incentives could weaken. Insufficient participation in validation could reduce the security of the network.

#### **9. Concentration of holdings**

If a large amount of zkVerify Tokens becomes concentrated in the hands of a small number of holders or entities, this could reduce decentralization. Large holders may exert

disproportionate influence over governance decisions, market liquidity, or staking dynamics, potentially distorting incentives or undermining network neutrality.

## **10. Governance**

zkVerify Token holders participate in the zkVerify protocol's governance. While decentralized governance enhances transparency, it may also lead to conflicting interests, voter apathy, or capture by well-organized minority groups. Disputes may result in delays to upgrades or even network splits (forks), potentially negatively affecting the value of zkVerify Tokens.

## **11. Integration and interoperability**

zkVerify's design includes interoperability with parachains and external systems. Reliance on third-party integrations or cross-chain bridges introduces additional risks, including vulnerabilities in external code and systemic risks from interconnected networks.

## **12. Reputation**

As with other emerging protocols, the perception of zkVerify is critical to adoption. Security incidents, governance disputes, or negative publicity involving associated entities could harm the protocol's reputation, reduce demand for zkVerify Tokens, and undermine long-term growth prospects of the entire zkVerify protocol.

## **13. Macroeconomics and environmental factors**

Broader macroeconomic conditions, such as monetary tightening or downturns in digital asset markets, can impact demand for zkVerify Tokens. In addition, while Proof-of-Stake systems are more energy-efficient than Proof-of-Work, negative perceptions about blockchain energy use generally could still affect sentiment towards the zkVerify protocol.

# **I.4 Project implementation-related risks**

## **1. Development**

zkVerify's architecture, which integrates the Relay Chain and parachain model, introduces complexity and interoperability challenges. Code vulnerabilities remain a risk, particularly because zkVerify supports on-chain upgrades that directly modify runtime logic. Errors in governance-approved upgrades could introduce bugs or unintended behaviors with systemic impact. The protocol also depends on the reliability of validators to maintain consensus and block finality. Validator downtime, collusion, or misbehavior could disrupt network operations or reduce security. Additionally, bridge protocols – that are necessary for connecting zkVerify with external blockchain ecosystems – are recognized as critical

cybersecurity risk vectors. Exploits of cross-chain bridges have historically led to significant asset losses across the industry, and zkVerify faces similar exposure.

## **2. Operation and execution**

The success of zkVerify depends on its broader ecosystem of Web2 and Web3 applications submitting zero-knowledge proofs for verification. Proof verifiers must be continuously updated and expanded to accommodate new proof systems. Faulty implementation or delays in updating verifiers could compromise verification accuracy and limit the protocol's utility, undermining confidence in zkVerify's core purpose.

## **3. Governance**

zkVerify employs an on-chain governance system in which zkVerify Token holders vote on proposals. While decentralized governance enhances transparency, it introduces risks of concentrated influence if a small number of large holders dominate voting power. This could lead to outcomes that favor narrow interests over the wider community. Governance disputes or manipulation may reduce stakeholder trust, while contentious decisions could result in chain splits (forks), fracturing the ecosystem and diminishing token value.

## **4. Markets and investors**

The zkVerify Token is not backed by reserves or intrinsic value guarantees. Its market price is speculative and subject to significant volatility driven by investor sentiment, macroeconomic trends, or crypto-asset market cycles. Periods of low activity or adverse market conditions may lead to reduced liquidity, widening spreads, resulting higher slippage for traders. Furthermore, token lockups and scheduled unlocks could release significant supply into the market, exerting downward pressure on price stability.

## **5. Partnerships and use-cases**

Adoption of zkVerify relies in part on partnerships with enterprises, application developers, and other blockchain ecosystems. If meaningful partnerships fail to materialize, or if anticipated use cases (such as cost-efficient proof verification) do not achieve adoption, the utility and perceived value of the zkVerify Token may diminish. Relying solely on organic community-driven growth could slow ecosystem expansion and limit adoption.

## **6. Continuity**

Ensuring continuity is critical for the reliability of zkVerify's core functions, including staking, governance, bridging, and relay chain operations. Prolonged downtime, technical failures, or governance deadlock could undermine user confidence and disrupt network activity. Moreover, zkVerify relies heavily on external contributors and infrastructure providers (e.g.

node operators, explorers, custodial integrations). Disruptions, service withdrawals, or security breaches affecting these external providers could directly impact operation.

## **7. Funding and resources**

The zkVerify Foundation currently funds much of the protocol's development and ecosystem growth. If financial resources are depleted faster than expected, or if future fundraising or ecosystem incentives prove insufficient, project development could slow. This dependency on sustained funding represents a risk to long-term sustainability.

## **8. Adoption and ecosystem growth**

zkVerify's long-term viability depends on attracting developers, projects, and users. Slow adoption, ecosystem fragmentation, or migration of projects to competing platforms could limit network effects and weaken the zkVerify Token's value proposition. In particular, if zkVerify does not achieve a critical mass of active verifiers and applications, it may struggle to maintain relevance against larger, established blockchain ecosystems.

# **I.5 Technology-related risks**

## **1. Relay Chain and parachains**

The zkVerify blockchain relies on the Relay Chain to coordinate parachains and validators. If the Relay Chain experiences instability – caused, for example, by software bugs, congestion or governance errors – parachains could fail to finalize blocks or process transactions. Because the ecosystem is interdependent, a failure in the Relay Chain may have cascading effects across all connected parachains, potentially leading to network-wide outages.

## **2. Interoperability**

zkVerify's design emphasizes interoperability between parachains and external networks. Failures in message queues or cross-chain coordination could result in incomplete or inconsistent transactions. In severe cases, this may lead to denial of service, loss of funds, or network partitioning, particularly for applications dependent on timely cross-chain data.

## **3. Runtime upgrades**

zkVerify supports on-chain governance for runtime upgrades. While this enables rapid innovation, it introduces risks if upgrades are not adequately tested or reviewed. Malicious proposals, rushed voting, or oversights in implementation could introduce vulnerabilities or cause unexpected behavior at the protocol level. Exploitation of these weaknesses may undermine network reliability or impact the security of the zkVerify Tokens.

#### **4. Validators and consensus**

The security of the zkVerify blockchain depends on a decentralized validator set. If a large number of validators go offline, collude, or act maliciously, block production could be disrupted, finality delayed, or chain reorganizations attempted. The nominators' role in selecting validators also creates risk – if nominators inadvertently delegate to malicious or Sybil-controlled validators, consensus integrity could be compromised.

#### **5. Bridges**

Bridges connecting one ecosystem to other ecosystems are historically among the most vulnerable components in blockchain networks. Exploits targeting bridge consensus, signature schemes, or message relaying could lead to token duplication, loss of assets, or disruption of cross-chain activity. A successful attack on a zkVerify bridge could damage trust in the ecosystem and reduce the security perception of the zkVerify Token.

#### **6. Upgrades and governance**

The ability to implement zero-downtime upgrades through governance is powerful but also dangerous. Automated or inadequately reviewed upgrades may unintentionally introduce critical bugs or be exploited through governance loopholes. Poor coordination during upgrades could lead to partial network outages or systemic malfunctions.

#### **7. Cryptography**

The zkVerify protocol relies on advanced cryptographic primitives for consensus, signatures, and zero-knowledge proof verification. If any of the underlying algorithms (e.g. Sr25519) were to be broken or weakened due to cryptographic advances or quantum computing, the security guarantees of the network and the zkVerify Token could be compromised.

#### **8. Nodes and network**

As a decentralized system, zkVerify depends on independent nodes to propagate transactions and maintain consensus. Network-level risks, such as denial-of-service (DoS) attacks, network partitioning, or targeted censorship, could impair functionality. If node operators run outdated or insecure software versions, the risks and vulnerabilities increase.

#### **9. Dependencies**

The zkVerify protocol is built on the Substrate framework and Polkadot technology stack. While these are mature and actively maintained, reliance on external codebases introduces dependency risks. Bugs, vulnerabilities, or governance decisions in upstream components could indirectly affect zkVerify's stability and performance.

## **I.6 Mitigation measures**

### **1. Consensus and validator safeguards**

The network is secured through a decentralized validator set distributed across multiple jurisdictions and operators, minimizing single points of failure. Validator integrity is enforced by staking economics: dishonest or underperforming validators are subject to slashing, which removes part of their staked zkVerify Tokens. This provides strong financial disincentives for malicious behavior. Token holders may nominate validators they trust, and nomination pools allow broader participation while diversifying risk. Validator performance – such as uptime and block finality – is continuously monitored, with underperforming validators rotated out automatically. These measures are used collectively to ensure that only reliable participants are able to take part in securing the Relay Chain.

### **2. Parachain and interoperability controls**

Only permissioned parachains may connect to the Relay Chain, ensuring that each parachain undergoes rigorous review before integration. Message queues between parachains are rate-limited, ordered, and securely processed to minimize congestion and reduce the risk of cross-chain inconsistencies. This design helps prevent service interruptions and denial-of-service conditions.

### **3. Governance and upgrade procedures**

On-chain upgrades follow a transparent governance process. Proposals are submitted publicly, undergo community referenda, and are subject to enactment delays, providing time for external audits, testing, and rollback in case vulnerabilities are discovered. Conviction-based voting – where longer token lockups increase voting weight – discourages short-term manipulation. Proposals may also be reviewed by technical collectives or fellowship groups with domain expertise, further reducing the likelihood of rushed or harmful upgrades.

### **4. Code quality testing and audits**

zkVerify's Substrate-based codebase is modular, allowing individual components (pallets) to be isolated, tested, and audited independently. Continuous integration and automated testing pipelines – including regression testing, fuzzing, and simulation – aim to catch vulnerabilities before deployment. Critical components undergo independent external audits before launch. The project also maintains a global bug bounty program, incentivizing white-hat researchers to identify and responsibly disclose vulnerabilities.

### **5. Bridge security measures**

Recognizing that bridges are high-value attack vectors, the zkVerify protocol employs light-client protocols for decentralized verification of cross-chain messages, removing reliance on third-party oracles. Bridges are subject to multiple external security audits prior to deployment. Where appropriate, multi-signature or threshold signature schemes are applied, ensuring no single party can unilaterally authorize transfers. These measures substantially reduce the risk of token duplication or cross-chain asset loss.

## **6. Cryptographic integrity**

zkVerify employs the Schnorrkel signature scheme, based on Ristretto, which is recognized for speed and robustness. To anticipate future threats, the zkVerify Foundation is actively researching quantum-resistant cryptographic standards. Regular audits of cryptographic implementations and peer-reviewed research partnerships further strengthen security.

## **7. Infrastructure redundancy and resilience**

The ecosystem avoids reliance on single service providers by promoting infrastructure diversity. Multiple community-maintained wallets (Polkadot.js, Nova, Talisman, SubWallet) and a range of RPC providers (ANKR, StakeFish, AntPool, Validation Cloud) ensure that no single tool becomes a systemic bottleneck. Indexing services such as SubQuery are open-source and widely deployed. As critical components are open source under permissive licenses, the community can fork and maintain them if the original providers withdraw.

## **8. Developer and ecosystem support**

The zkVerify Foundation provides grants, documentation, workshops, and technical support to encourage best practices in development. By building and encouraging a knowledgeable and resilient developer community, the likelihood of insecure or poorly implemented parachains, verifiers, or integrations is reduced.

## **9. Incident response**

In addition to preventative measures, structured incident response processes are maintained. This includes community-driven governance mechanisms for rapid emergency upgrades, transparent disclosure of critical vulnerabilities when appropriate, and treasury funding for emergency fixes, focusing on timely mitigation if risks materialize.

## **Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts**

### **J.1 Adverse impacts on climate and other environment-related adverse impacts**

#### **S.1 Name**

zkVerify Foundation

#### **S.2 Relevant legal entity identifier**

254900YN0N9Y7NYQTF19

#### **S.3 Name of the crypto-asset**

zkVerify Token (VFY)

#### **S.4 Consensus Mechanism**

The zkVerify blockchain employs a hybrid consensus mechanism that combines BABE (Blind Assignment for Blockchain Extension) for block production with GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) for finality.

BABE is a Proof-of-Stake –based protocol that uses a lottery mechanism to determine which validator may produce the next block. The probability of being selected is weighted by the amount of the validator’s stake, similar in design to the Ouroboros protocol used by Cardano. This ensures continuous block production and fair participation among validators.

GRANDPA, by contrast, provides strong finality. It is a Byzantine Fault Tolerant (BFT) protocol in which validators vote on the “head” of the chain. Once at least two-thirds of the validators attest to a specific chain, all blocks up to that point are finalized and cannot be reverted. This separation between block production (with BABE) and finality (with GRANDPA) enables the zkVerify blockchain to achieve both efficiency and strong security guarantees.

The consensus mechanism of zkVerify is designed to be robust and secure under standard fault tolerance assumptions. It can tolerate up to one-third of validators behaving maliciously without losing finality, which is the standard threshold for BFT protocols. If more

than one-third, but fewer than half of, validators act maliciously, block finality may temporarily halt. However, BABE can continue producing blocks with probabilistic finality until GRANDPA resumes. In the extreme case where an attacker would control a majority of stake (i.e. 51% or more), they could disrupt consensus. To counter this, zkVerify incorporates economic safeguards – most notably slashing of misbehaving validators’ stakes – which impose severe financial penalties on malicious actors, thereby deterring such attacks.

To further strengthen security, zkVerify organizes consensus participation into sessions: short intervals during which validator assignments and responsibilities are rotated. This frequent rotation of GRANDPA authorities makes it significantly harder for an adversary to predict or corrupt validator sets, enhancing both decentralization and resilience.

## **S.5 Incentive Mechanisms and Applicable Fees**

As mentioned in Section [H.3](#) above, the zkVerify blockchain secures transactions through a NPoS consensus mechanism. In this system, validators are responsible for producing blocks and verifying transactions, while nominators (i.e. the token holders who delegate their stake to validators) support the validator set and share in the rewards.

Validators earn token rewards through a combination of inflationary issuance and a share of collected transaction fees. Nominators receive a proportional share of these rewards based on the performance of the validators they support. To preserve network integrity, the protocol applies slashing penalties in cases of malicious activity, such as double-signing or collusion, as well as for prolonged validator downtime. Both validators and their nominators are subject to these penalties, aligning incentives toward honest and reliable participation.

Transaction fees, paid in zkVerify Tokens, are calculated using a weight-based fee model. Each transaction includes a base fee, an additional fee determined by the computational complexity (weight) of the transaction, and a size-related fee based on the number of bytes transmitted. Fees are dynamically adjusted by a congestion multiplier, which increases or decreases costs depending on current network demand. This mechanism helps prevent spam, ensures throughput efficiency, and maintains predictable network performance.

A portion of collected fees is allocated to the zkVerify Treasury, which supports ecosystem development, protocol maintenance, and governance initiatives. All incentive and fee structures are embedded directly into the protocol logic, ensuring transparent and decentralized distribution without reliance on centralized control.

## **S.6 Beginning of the period to which the disclosed information relates**

2024-09-01

## **S.7 End of the period to which the disclosed information relates**

2025-09-01

## **S.8 Energy consumption**

82000.00000 kWh/a

## **S.9 Energy consumption sources and methodologies**

As the zkVerify blockchain's mainnet has not yet launched, direct energy consumption measurements are not available. Accordingly, the figures provided are based on transparent assumptions and comparisons with existing Proof-of-Stake (PoS) networks that share a similar architecture and hardware profile. The methodology follows the approach adopted by the Crypto Carbon Ratings Institute (CCRI) in its assessments of PoS blockchain protocols, which estimate per-node electricity draw and extrapolate to network totals based on validator and full-node counts. CCRI's 2022 study measured the energy use of Polkadot – another Substrate-based relay chain – and found that a typical node consumed approximately 27 watts continuously, equivalent to ~236.5 kWh per year. With ~297 nodes active, Polkadot's total annual energy consumption was calculated at ~76,807 kWh.<sup>1</sup>

Using this benchmark as a proxy, zkVerify's projected consumption was derived by multiplying the per-node estimate by assumed node counts at launch (200–600 validators and supporting nodes) and applying a 15% overhead to account for ancillary services such as RPC endpoints, monitoring infrastructure, and explorers. For context, these figures were cross-checked against CCRI's more recent assessments of other PoS networks. Cardano was estimated to consume approximately 687,238 kWh annually (2024)<sup>2</sup>, while post-Merge Ethereum consumed ~2.6 million kWh annually (2022)<sup>3</sup>. Solana's reported consumption is higher still, at ~8.8 million kWh annually (2024)<sup>4</sup>. These comparisons confirm that zkVerify's

---

<sup>1</sup> PoS Benchmark Study 2023 - Energy Efficiency and Carbon Footprint of PoS Blockchain Networks and Platforms (<https://carbon-ratings.com>).

<sup>2</sup> MiCA-compliant sustainability indicators for the Cardano Network (<https://carbon-ratings.com>).

<sup>3</sup> The Merge - Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network (<https://carbon-ratings.com>).

<sup>4</sup> <https://solana.com/news/energy-use-report-september-2024>.

projected annual consumption of ~82,000 kWh falls within the expected range for small-to-mid-sized PoS relay chains and is substantially lower than that of larger PoS networks.